

## 1)SERVER ACCESS LOGGING

## TO GET THE LOGS FOR OUR STATIC WEBSITE HOSTED IN BUCKET

## Step II : Click on Properties.

Step IV : Select Destination where we want to store the logs and click on Save Changes tab.

[illegible]

## 2)HOW TO CHANGE OBJECT OWNERSHIP

If you didn't set up ACL when making the bucket, you can't turn it later by editing the Access Control List to solve this Issue, we can simply change the object ownership.

Step I : Go to Permissions and enabled the ACL .

Step II : choose object Ownership .

Step III : and simply click on save changes.

The screenshot shows the 'Edit Object Ownership' page in the Amazon S3 console. The breadcrumb trail at the top reads: Amazon S3 > Buckets > sweetbucket > Edit Object Ownership. The page title is 'Edit Object Ownership' with an 'Info' link. Below the title is a section titled 'Object Ownership' with a description: 'Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.'

There are two radio button options for 'Object Ownership':

- ☐ ACLs disabled (recommended)  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ☒ ACLs enabled  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Below these options are two yellow warning boxes:

- The first box states: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.'
- The second box is titled 'Enabling ACLs turns off the bucket owner enforced setting for Object Ownership'. It explains that once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. It also states: 'Access to objects that you do not own will be based on ACLs and not the bucket policy.' Below this text is a checked checkbox: 'I acknowledge that ACLs will be restored.'

Below the warning boxes, there are two radio button options for 'Object Ownership':

- ☒ Bucket owner preferred  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
- ☐ Object writer  
The object writer remains the object owner.

At the bottom of the page, there is a blue information box with a question mark icon: 'If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)'.

At the very bottom of the page, there are two buttons: 'Cancel' and 'Save changes'.

### 3)REQUESTER PAYS

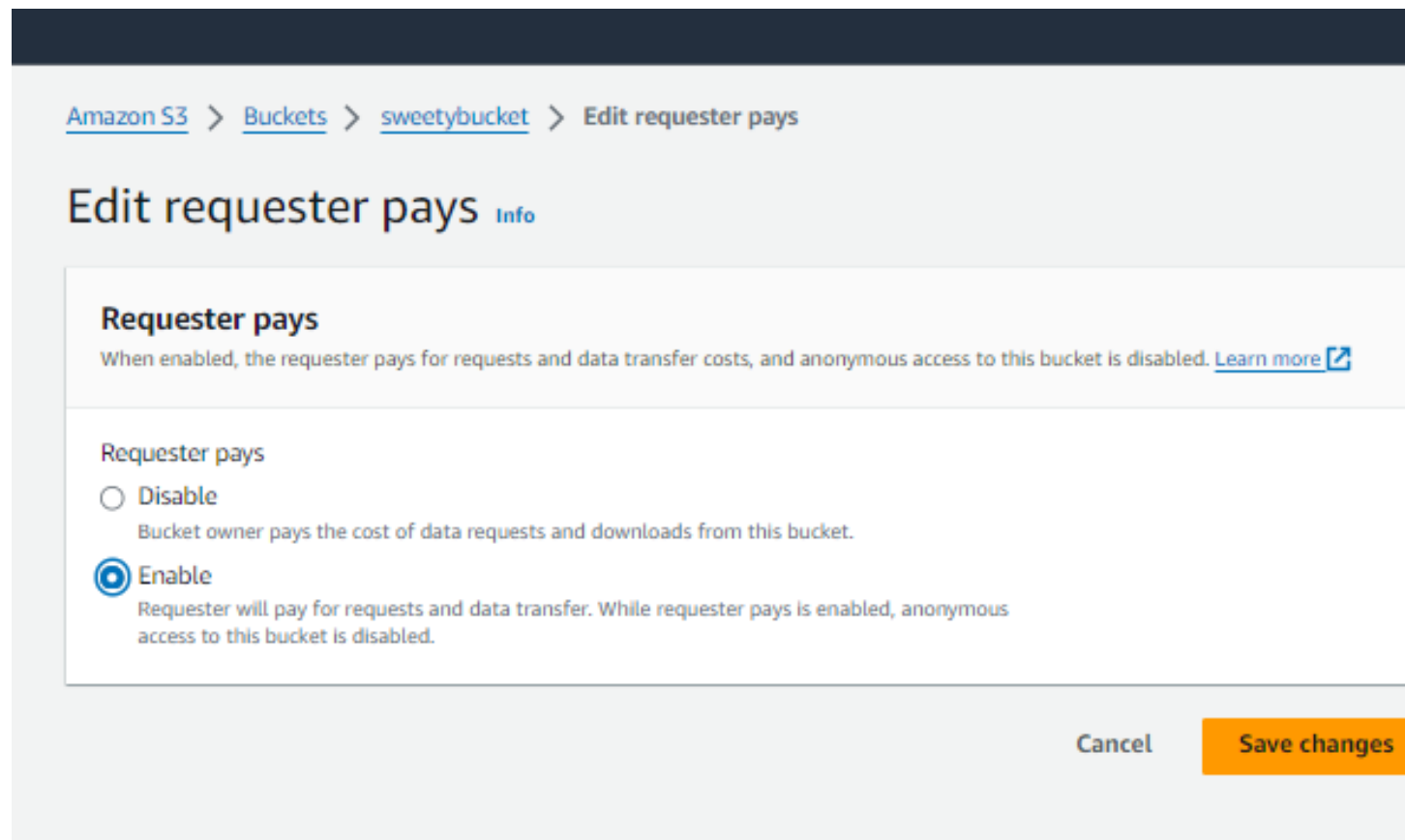
When we enable the Requester Pays in AWS , the people who want to access your data they pay for it, not owner.

Step I : Select Bucket and go to Properties .

Step II : Find Requester Pays Option .

Step III : Select Edit to enable it .

Step IV : then Save Changes.



The screenshot shows the AWS console interface for editing the 'Requester Pays' setting on a bucket named 'sweetybucket'. The breadcrumb trail at the top reads: [Amazon S3](#) > [Buckets](#) > [sweetybucket](#) > [Edit requester pays](#). The main heading is 'Edit requester pays' with an 'Info' link. Below this, a section titled 'Requester pays' contains a descriptive paragraph: 'When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)'. There are two radio button options: 'Disable' (unselected) and 'Enable' (selected). The 'Enable' option has a sub-description: 'Requester will pay for requests and data transfer. While requester pays is enabled, anonymous access to this bucket is disabled.' At the bottom right, there are two buttons: 'Cancel' and 'Save changes'.

[Amazon S3](#) > [Buckets](#) > [sweetybucket](#) > [Edit requester pays](#)

## Edit requester pays [Info](#)

**Requester pays**

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

☐ Disable  
Bucket owner pays the cost of data requests and downloads from this bucket.

☒ Enable  
Requester will pay for requests and data transfer. While requester pays is enabled, anonymous access to this bucket is disabled.

[Cancel](#) [Save changes](#)

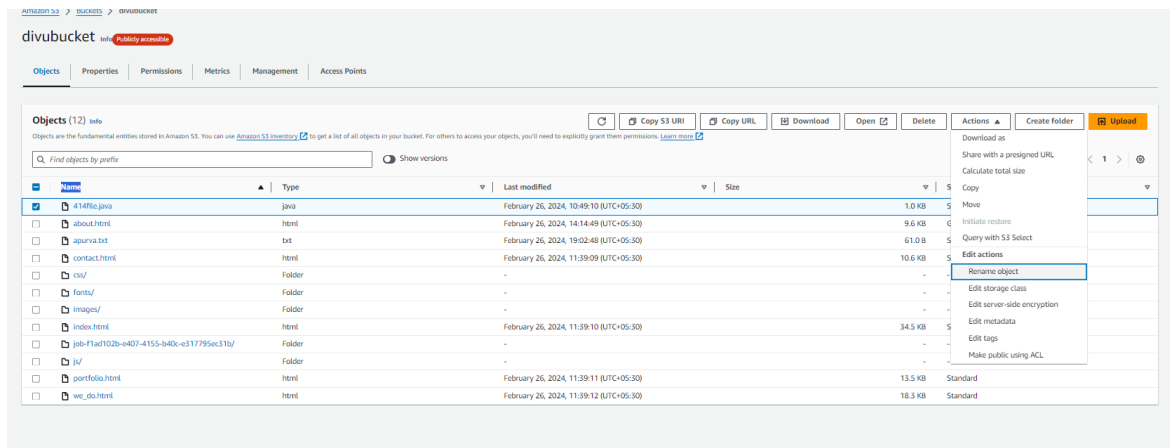
## 4) ACTIONS PERFORMED ON BUCKET OBJECTS.

Using actions on AWS, we can perform copy, move, rename, change storage class on object.

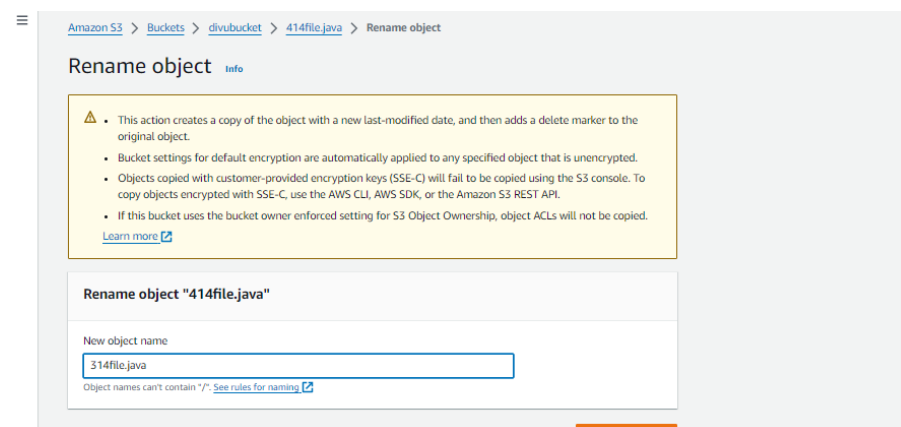
### 1)FOR RENAME

Step I : Select Object in Bucket.

Step II : Choose the Action rename from menu.



Step III : Rename it and change changes.



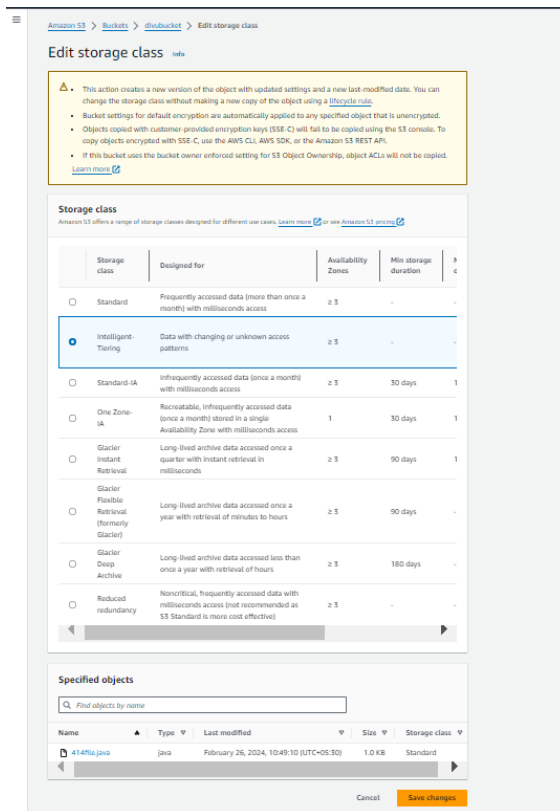
### 2)FOR CHANGE STORAGE CLASS

Step I : Select Object in Bucket.

Step II : Choose the Action Storage class from menu.

Step III : Select the Storage which you want.

Step IV : Save Changes.

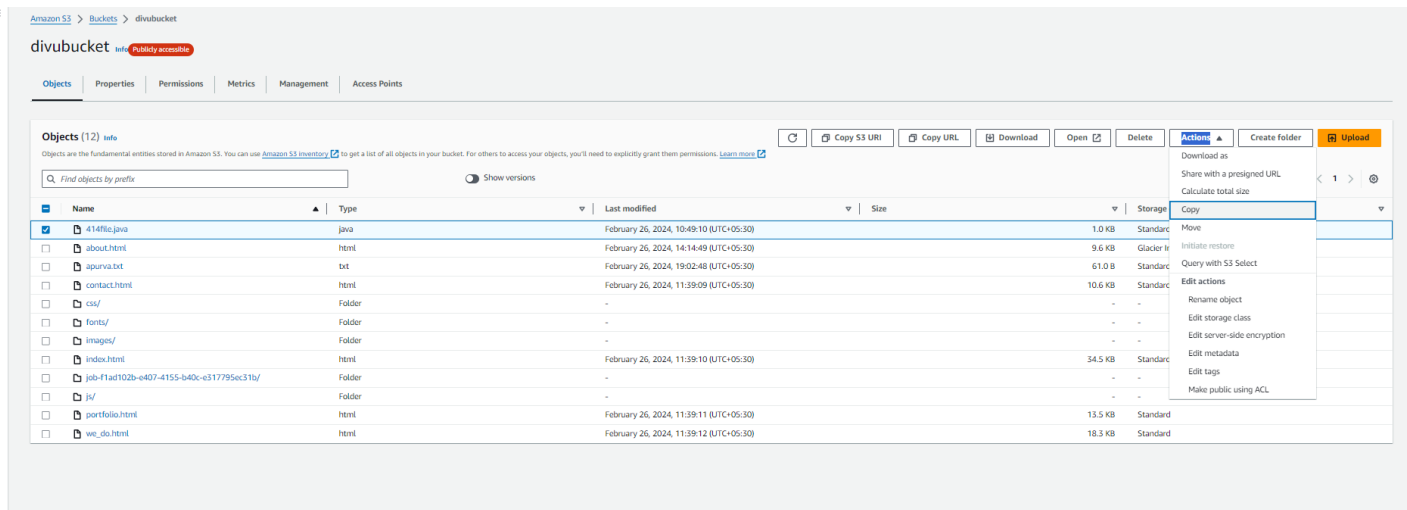


### 3)COPY

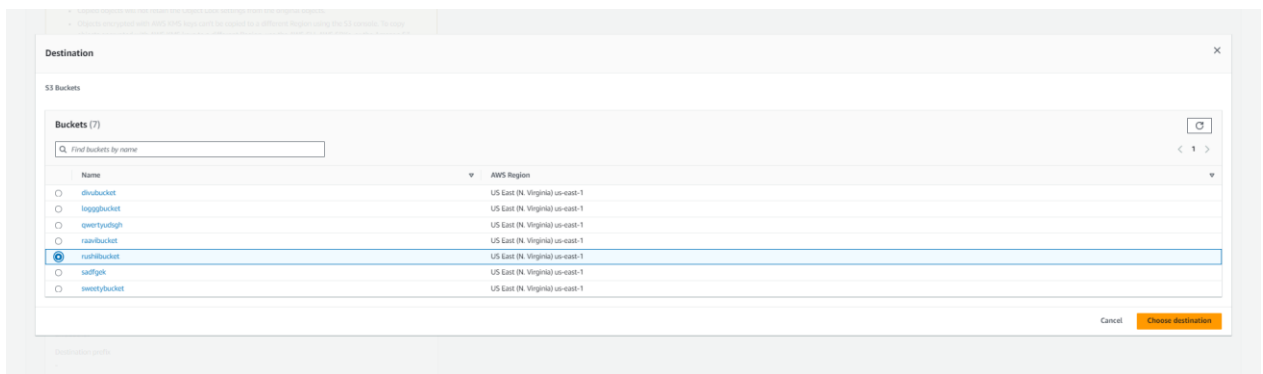
Copy means create duplicate of original file

Step I : Select the object in Bucket.

Step II : Choose the Action Copy from menu.



Step III : Select the Destination.



Step IV : and click on Copy.

**Copy**

**Warning:** This action creates a copy of the object with updated settings and a new last-modified date. This action applies to all objects within the specified folders (prefixes). Objects added to these folders while the action is in progress might be affected.

- Copied objects will not retain the Object Lock settings from the original objects.
- Objects encrypted with AWS KMS keys can't be copied to a different Region using the S3 console. To copy objects encrypted with AWS KMS keys to a different Region, use the AWS CLI, AWS SDKs, or the Amazon S3 REST API.
- Objects encrypted with customer-provided encryption keys (SSE-C) will fail to be copied using the S3 console. To copy objects encrypted with SSE-C, use the AWS CLI, AWS SDKs, or the Amazon S3 REST API.
- If the bucket you are copying objects from uses the bucket owner enforced setting for S3 Object Ownership, object ACLs will not be copied to the specified destination.
- If you want to copy objects to a bucket that uses the bucket owner enforced setting for S3 Object Ownership, you'll need to ensure that the source bucket also uses the bucket owner enforced setting or object ACL grants to other AWS accounts and groups have been removed.

[Learn more](#)

**Destination**

Destination type  
☒ General purpose bucket  
☐ Directory bucket  
☐ Access Point

Destination  
 [View](#) [Browse S3](#)

From: s3://ru01bucket  
 Destination bucket name  
 ru01bucket  
 Destination prefix  
 -

**Destination details**

The following bucket settings impact new objects stored in the specified destination.

Bucket Versioning	Default encryption type	Object Lock
Other enabled, multiple variants of an object can be stored in the bucket. To verify supported features, see <a href="#">Object Lock</a> and <a href="#">Bucket Versioning</a> .	Bucket settings for default encryption are automatically applied to any specified object that is overwritten.	When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely.
Enabled	Server-side encryption with Amazon S3 managed keys (SSE-S3)	Disabled

[Learn more](#)

**Specified objects**

Name	Type	Last modified	Size
+14file.java	java	February 26, 2024, 10:49:10 (UTC+05:30)	1.0 KB

**Checksums**

Checksum functions are used for additional data integrity verification of new objects. [Learn more](#)

**Additional checksums**

☒ Copy existing checksum functions  
 Apply the same checksum function to the destination object. The checksum value may change compared to when it was added. [Learn more](#)

☐ Replace with a new checksum function  
 Specify a new checksum function for additional data integrity validation which will overwrite any existing data integrity settings.

Cancel Copy

## 4)MOVE

Move means transfer file from one location to another

It like Cut + Paste.

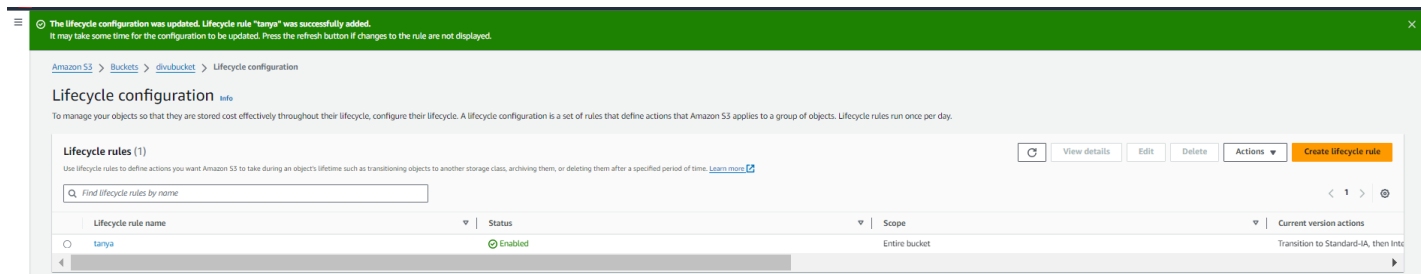
## 5)LIFECYCLE RULE

Lifecycle rule in AWS automatically manages the objects by performing tasks like changing storage class, expiring objects based on rules which you set.

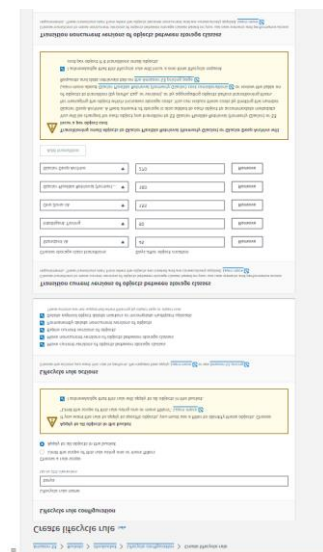
Step I : Select the bucket name .

Step II : Click on Management .

## Step III : Click on create lifecycles rules.



## Step IV : Give the rule name, choose scope ,select Actions, expiry and conditions



## Step V : Click on create rule.





## Step III : Click on create replication rule.

Replication rules (1)											
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. <a href="#">Learn more</a>											
	Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync
<input type="radio"/>	wall	Enabled	s3://raavibucket	US East (N. Virginia) us-east-1	0	Entire bucket	Same as source	Same as source	Disabled	Do not replicate	Disabled
<a href="#">View replication configuration</a>											

## Step IV : Give the name to replication rule, select Status, define source and Destination.

### Create replication rule

#### Replication rule configuration

Replication rule name

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

☒ Enabled

☐ Disabled

Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

1

#### Source bucket

Source bucket name

dnubucket

Source Region

US East (N. Virginia) us-east-1

Choose a rule scope

☒ Limit the scope of this rule using one or more filters

☐ Apply to all objects in the bucket

#### Tags

You can limit the scope of this rule to the key value pairs added below.

#### Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Single-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#)

☒ Choose a bucket in this account

☐ Specify a bucket in another account

Bucket name

Choose the bucket that will receive replicated objects.

Destination Region

US East (N. Virginia) us-east-1

The IAM role associated with this configuration might not have the correct permissions for this new destination bucket. You must create a new IAM role or update the permissions associated with the existing role in the IAM console.

## Step V : after all settings click on Saves.

## Destination storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

☐ Change the storage class for the replicated objects

## Additional replication options

☐ Replication Time Control (RTC)

Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. [Learn more](#)

☐ Replication metrics

With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. [Learn more](#) or see [Amazon CloudWatch pricing](#)

☐ Delete marker replication

Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. [Learn more](#)

☐ Replica modification sync

Replicate metadata changes made to replicas from the destination bucket to the source bucket. [Learn more](#)

Cancel

Save

Step VI : Here ,Replication is generated.

Replication rules (2)											
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. <a href="#">Learn more</a>											
<div><div></div><div>View details</div><div>Edit rule</div><div>Delete</div><div>Actions</div><div>Create replication rule</div></div>											
<div>&lt; 1 &gt; ⌂</div>											
	Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync
<input type="radio"/>	shiv	Enabled	s3://rushibucket	US East (N. Virginia) us-east-1	1	Prefix: a	Same as source	Same as source	Disabled	Do not replicate	Disabled
<input type="radio"/>	wall	Enabled	s3://raavibucket	US East (N. Virginia) us-east-1	0	Entire bucket	Same as source	Same as source	Disabled	Do not replicate	Disabled

## 6)INVENTORY RULES

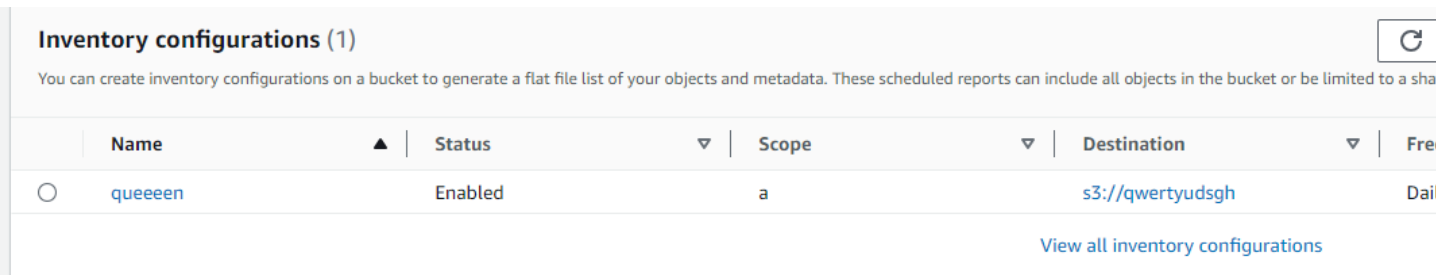
Inventory rule generate the report on the objects stored in S3 bucket.

It gives detailed information about metadata, size, storage class,etc.

Step I : Step I : Select the bucket name .

Step II : Click on Management .

Step III : Click on create Inventory rule.



The screenshot shows the 'Inventory configurations (1)' page in the AWS IAM console. It includes a table with one configuration named 'queeeen' which is 'Enabled' and has a scope of 'a'. The destination is 's3://qwertyudsg'. A link 'View all inventory configurations' is at the bottom right.

Inventory configurations (1)					
You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a sha					
	Name ▲	Status ▼	Scope ▼	Destination ▼	Fre
<input type="radio"/>	queeeen	Enabled	a	s3://qwertyudsg	Dai
<a href="#">View all inventory configurations</a>					

Step IV : Give Inventory Configuration name, Scope, report details ,choose destination which bucket we want the report.

## Create inventory configuration Info

### Inventory configuration name

Inventory configuration name

The name can contain up to 64 characters using letters, numbers, underscores, periods, or dashes.

### Inventory scope

**Prefix - optional**  
Limit the scope of this configuration to a single prefix.

Don't include the bucket name in the prefix.

**Object versions**

☒ Current version only

☐ Include all versions

### Report details

**Destination bucket**  
Choose the destination bucket where you want reports to be saved. The destination bucket must be in the same AWS Region as the source bucket. [Learn more](#)

☒ This account

☐ A different account

**Destination**  
Choose or enter the destination bucket that will receive the inventory reports.

Format: s3://<bucket>/<optional-prefix-with-path>

**Destination bucket permission**  
The following statement will be added to the destination bucket policy to allow Amazon S3 to place data in that bucket. [Learn more](#)

```
{
  "Sid": "InventoryAndAnalyticsExamplePolicy",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
```

Step V : Select the metadata fields and click on create.

```
{
  "Sid": "InventoryAndAnalyticsExamplePolicy",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
```

**Frequency**  
Choose how often the report will be generated.

☒ Daily  
The first report will be delivered within 48 hours.

☐ Weekly  
The first report will be delivered within 48 hours and subsequent reports will be delivered on Sundays.

**Output format**  
Choose the output format based on the number of objects that you expect to list or the analysis tool that you want to use. [Learn more](#)

☒ CSV  
Choose this format if you plan to use Batch Operations or if you plan to analyze S3 inventory with tools like Microsoft Excel.

☐ Apache ORC

☐ Apache Parquet

**Status**  
Choose whether the configuration will be enabled to publish inventory reports.

☐ Disable

☒ Enable

### Inventory report encryption Info

Server-side encryption protects data at rest.

**Server-side encryption**

☒ Do not specify an encryption key  
The bucket's default encryption is used to encrypt objects when storing them in Amazon S3.

☐ Specify an encryption key  
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

**Warning:** If the bucket policy for the specified destination requires objects to be encrypted before storing them in S3, you must specify an encryption key or storing your inventory report in the destination will fail.

### Additional metadata fields - optional

Choose the metadata that should be included for each listed object in the report. [Learn more](#)

**Object**

☒ Size

☒ Last modified

☒ Metadata updated

☒ Replication status

☒ Encryption

☒ Bucket key status

**Permissions**

☒ Object ACL

☒ Object owner

**Storage class**

☒ Storage class

☒ Intelligent Tiering Access tier

**Data integrity**

☒ ETag

☒ Additional checksums function

**Object Lock**

☒ All Object Lock configurations

- ☐ Object Lock: Retention mode
- ☐ Object Lock: Retain until date
- ☐ Object Lock: Legal hold status

# Step VI : here, Inventory rule is generated.

✔ Inventory report1 successfully created.  
It may take up to 48 hours to deliver the first report.

ⓘ No modifications were made to the destination bucket policy  
A valid bucket policy for writing to the destination bucket already exists.

Amazon S3 > Buckets > divubucket > Management > Inventory configurations

Inventory configurations (2) Info

↻

View details

Edit

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

	Name ▲	Status ▼	Scope
<input type="radio"/>	queeeen	Enabled	a
<input type="radio"/>	report1	Enabled	Entire